Автор:
Белей Євгеній Володимирович
студент 4 курсу
спеціальності 014 Середня освіта (Інформатика)
факультету математики, інформатики та фізики
Науковий керівник:
Франчук Наталія Петрівна,
кандидат педагогічних наук, доцент

ПРОБЛЕМИ БЕЗПЕКИ ПІД ЧАС ХМАРНИХ ОБЧИСЛЕНЬ

Анотація. Розглядаються основні загрози безпеці хмарних обчислень та методи їх захисту, що ґрунтуються на стандартах та рекомендаціях міжнародних організацій, таких як: Cloud Security Alliance (CSA) та National Institute of Standards and Technology (NIST).

Ключові слова: хмарні обчислення, обчислювальні ресурси, загрози безпеці хмарних обчислень, стандарти захисту.

Вступ. Застосування хмарних обчислень надають користувачам та організаціям доступ до потужних обчислювальних ресурсів та сховищ даних через мережу Інтернет. Зокрема у статті [6] детально розглядають деякі приклади використання хмарних обчислень для навчальних цілей (обчислення наближеного значення подвійного інтеграла; розв'язування графічних двовимірних задач; знаходження найменшого значення опуклої спадної функції та ін. Науковець Чао Лі (Chao Lee) [1] розглядає багато питань (хмаро орієнтоване середовище навчання, хмарні лабораторії, практичне навчання, персональне навчальне середовище, мобільне навчання тощо) серед яких й питання безпеки у хмарі. Адже хмарні обчислення також пов'язані з низкою загроз безпеці, таких як порушення конфіденційності, цілісності та доступності даних, а також недостатній контроль над хмарною інфраструктурою та службами.

Мета дослідження. Проаналізувати основні загрози безпеці хмарних обчислень та існуючі рішення для їх запобігання.

Основна частина. Серед багатьох загроз безпеці хмарних обчислень можна виокремити такі основні: порушення конфіденційності даних; порушення цілісності даних; порушення доступності даних та служб [2]. Розглянемо їх детальніше.

Порушення конфіденційності даних. Ця загроза пов'язана з незаконним доступом до даних користувачів або організацій, що розміщені у хмарі. Порушення конфіденційності може статися через: атаку зловмисників на канали зв'язку або сховища даних у хмарі; недостатній захист даних шифруванням або автентифікацією; помилки або зловживання CSP або інших сторонніх служб; неправильне налаштування політик доступу; витік даних; спільно використовувані ресурси у хмарі. Порушення конфіденційності може призвести до шкоди для репутації, конкурентоспроможності чи фінансового становища користувачів або організацій, а також порушення законодавства щодо захисту персональних даних.

Порушення цілісності даних. Ця загроза пов'язана з незаконною зміною або пошкодженням даних користувачів або організацій у хмарі. Порушення цілісності може статися через: атаку зловмисників на дані в хмарі; помилки або зловживання CSP або інші сторонні служби; неправильне настроювання політик резервного копіювання або відновлення даних; технічний збій або помилки в хмарі. Порушення цілісності може призвести до втрати або спотворення важливих даних, а також порушення функціонування додатків або служб у хмарі.

Порушення доступності даних та служб. Дана загроза пов'язана з неможливістю доступу до даних або служб у хмарі з причин, що не залежать від користувачів чи організацій. Порушення доступності може статися через: атаку зловмисників на хмарну інфраструктуру або служби, наприклад, атаки відмови в обслуговуванні (DoS) або розподілену атаку відмови в обслуговуванні (DDoS); помилки або зловживання CSP або

інших сторонніх служб; неправильне налаштування політик масштабування або балансування навантаження; технічні збої або помилки в хмарі. Порушення доступності може призвести до зниження продуктивності або простою програм або служб у хмарі, а також до втрати довіри з боку користувачів чи організацій.

Для вирішення проблем безпеки хмарних обчислень використовуються ефективні механізми та методи захисту, які враховують специфіку хмарної моделі та задовольняють вимоги користувачів та організацій. Вони відповідають стандартам та рекомендаціям щодо захисту хмарних обчислень, розробленим міжнародними організаціями, такими як: Cloud Security Alliance (CSA) та National Institute of Standards and Technology (NIST). Cloud Security Alliance (CSA) – це некомерційна організація, яка об'єднує експертів з безпеки хмарних обчислень з кожної галузі, а також рекомендації щодо їх вирішення з використанням кращих практик та стандартів. National Institute of Standards and Technology (NIST) – це агентство уряду США, що займається розробкою та встановленням стандартів та метрик у різних галузях науки та технологій. NIST також бере активну участь у розвитку стандартів та рекомендацій з безпеки хмарних обчислень, таких як:

– *NIST Special Publication 800-144*: Guidelines on Security and Privacy in Public Cloud Computing [3]. Цей документ містить посібники з безпеки та конфіденційності даних у публічних хмарах, які призначені для користувачів та організацій, що використовують або планують використовувати хмарні служби. Посібники охоплюють такі аспекти, як визначення ролей та відповідальності з безпеки у хмарі, вибір відповідного типу та моделі хмари, оцінка ризиків безпеки хмари, застосування контрольних заходів безпеки хмари, дотримання законодавчих та регуляторних вимог щодо захисту даних у хмарі та інші.

– *NIST Special Publication 800-145*: NIST Definition of Cloud Computing [4]. Цей документ містить офіційне визначення хмарних обчислень від NIST, яке широко використовується у науковій та практичній літературі. Визначення описує основні характеристики хмарних обчислень. Також визначення класифікує хмарні обчислення за трьома критеріями: типом хмари (публічна, приватна, гібридна або громадська), моделі служби (IaaS, PaaS або SaaS) та моделі розгортання (на місці, поза місцем або комбінована).

– *NIST Special Publication 800-146*: Cloud Computing Synopsis and Recommendations [5]. Цей документ містить короткий огляд основних концепцій та термінів хмарних обчислень, а також рекомендації щодо застосування хмарних обчислень у різних сценаріях. Рекомендації стосуються таких питань, як вибір відповідного типу та моделі хмари для конкретного робочого навантаження, оцінка витрат та вигоди від переходу в хмару, управління життєвим циклом даних у хмарі, управління безпекою та конфіденційністю даних у хмарі, управління контрактами та відносинами з CSP та інші.

Висновки. Безпека хмарних обчислень є актуальною та важливою темою для розвитку та розповсюдження хмарних технологій. Для гарантування безпеки хмарних обчислень необхідно застосовувати комплексний та системний підхід, який враховує специфіку хмарної моделі та вимоги користувачів та організацій. Також необхідно стежити за появою нових загроз і рішень безпеці хмарних обчислень та адаптуватися до середовища, що змінюється. Безпека у хмарі є загальною відповідальністю всіх учасників: користувачів, організацій та CSP.

Список використаних джерел:

1. Chao Lee. (2016). Handbook of Research on Cloud-Based STEM Education for Improved Learning Outcomes. URL: http://www.igi-global.com/book/handbook-researchcloud-based-stem/140984#table-of-contents. DOI: https://doi.org/10.4018/978-1-4666-9924-3.

2. Cloud Security Alliance. (2019). The Treacherous 12: Cloud Computing Top Threats in 2016. URL: https://downloads.cloudsecurityalliance.org/assets/research/top-threats/Treacherous-12_Cloud-Computing_Top-Threats.pdf

3. National Institute of Standards and Technology. (2011). NIST Special Publication 800-144: Guidelines on Security and Privacy in Public Cloud Computing. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf

4. National Institute of Standards and Technology. (2011). NIST Special Publication 800-144: Guidelines on Security and Privacy in Public Cloud Computing. URL: https://csrc.nist.gov/publications/detail/sp/800-145/final

5. National Institute of Standards and Technology. (2012). NIST Special Publication 800-144: Guidelines on Security and Privacy in Public Cloud Computing. URL: https://csrc.nist.gov/publications/detail/sp/800-146/final

6. Zhaldak, M.I., Franchuk, V.M., and Franchuk, N.P. (2021). Some applications of cloud technologies in mathematical calculations. Journal of Physics: Conference Series **1840** 012001. URL: https://iopscience.iop.org/article/10.1088/1742-6596/1840/1/012001. DOI: https://doi.org/10.1088/1742-6596/1840/1/012001.